REMARKS

STATUS OF THE CLAIMS

Claims 1-26 are pending in the application.

Claims 1-6, and 16-26 were rejected under 35 U.S.C. 103(a) as being unpatentable over Yasukawa et al. (U.S. 5,999,622) in view of Rhoads (U.S. 6,343,138), in view of Millsted et al. (U.S. 6,263,313), and further in view of Stefik et al. (U.S. 6,233,684).

Claims 7-15 were rejected under 35 U.S.C. 103(a) as being unpatentable over Yasukawa/Rhoads/Millsted/Stefik in view of Applicant's own admission.

Claims 1-26 remain pending, reconsideration of which is respectfully requested in view of the clarifying remarks herein.

REJECTIONS

Claims 1-6 and 16-26

The independent claims are 1, 25 and 26, which are rejected as being unpatentable over a combination of Yasukawa, Rhoads, Millsted and Stefik

Yasukawa discloses that only some segments of a file are encrypted. It also discloses that by obtaining a decryption key from a key distribution center and setting the decryption key in a decryption virtual device driver, a bit map table showing how an encrypted portion is encrypted is extracted and the encrypted portion is decrypted using the obtained decryption key.

Yasukawa originally assumes that data is stored in recording medium such as CD-ROMs. In order to store encrypted data into Yasukawa's recording medium, a decryption key is required separately, or media-specific information can be used as an encryption key. Yasukawa discloses the former case, but it involves a problem of losing a key, which is at least one problem that the present invention tries to solve. In the latter media-specific case, a problem arises that even an authorized user cannot use a digital content file stored in recording media when the digital data is copied to another recording medium.

Also, because no processing is performed on a non-encrypted part 46 in Yasukawa, it differs from what the present invention claims, that is "***embedding user-specific authorization information***, containing information ***for accessing the encrypted digital content file***, as

invisible information in the extracted preview sample to prepare a user-specific-authorization-information-embedded preview sample" (e.g., claim 1). The Office Action newly alleges in page 4, that it would have been obvious to modify Yasukawa to encrypt just a sample of the data file and reinsert the encrypted section into the data file, because it allows digital information to be copied and distributed easily over a wide variety of mediums, including modems, wireless technologies, CD-ROMs, floppy disks, the Internet, bulleting boards, computer networks, while preventing unauthorized use of the data.

MPEP §706.02(j) sets forth a guideline on the contents of a rejection under §103: "To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure" (emphasis in original). *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP 2143-2143.03 for decisions pertinent to each of these criteria. Factual findings in support of a *prima facie* case of obviousness must be supported by substantial evidence. In re Zurko, 59 USPQ2d 1693, 1696 (Fed. Cir. 2001).

First, there is no motivation in Yasukawa itself to be modified to encrypt just a sample, based upon the modification motivation rationale relied upon by the Office Action, because considering Yasukawa entirely, Yasukawa relates to "sector-based decryption in the file system of a computer operating system" (column 1, lines 7-10), so that contrary to the Office Action suggestion, there would be no motivation to modify Yasukawa for distribution via network technologies. It is readily apparent that Yasukawa is drawn to storage mediums, such as a CD-ROM and the like, uses a volume bitmap table (VBT) (FIGS. 6-8 and column 3, line 65 to column 4, line 5), which is used in connection with storage mediums, but not for network transmission/reception. Further, a review of the entire Yasukawa reveals that there is no disclosure or suggestion to perform any processing on the non-encrypted part (preview part) 46. So the Office Action relies on knowledge of one skilled in the art to modify Yasukawa. However, one skilled in the art would not encrypt the non-encrypted parts 46, because it would frustrate

previewing by a user, as suggested by Yasukawa in column 4, lines 16-29 and contrary to the Office Action's suggestion it would not accommodate easy distribution. It is readily apparent that the Office Action's motivation rationale to modify Yasukawa to encrypt just a sample of the data file (page 4 of the Office Action) is hereby traversed.

So the Office Action relies on Rhoads, which discloses a method to hide an identification code signal in a carrier signal. Yasukawa is directed to a method to encrypt a file to be stored in the recording medium, such as CD-ROMs. Therefore, there would have been no motivation in Rhoads, which is directed to a method to hide the identification code signal in a carrier signal as mentioned earlier, to be combined with Yasukawa, because Yasukawa already protects data on a storage medium using encryption. Significantly, however, there is no motivation in Rhoads or there would be no motivation in knowledge of one skilled in the art to use Rhoads' use of hidden data in a non-encrypted preview portion of Yasukawa's information 36, because Rhoads' is drawn to methods of hiding identification code signal in a carrier signal, and not to describing range of uses of such hidden data. In other words, a review of Rhoads fails to suggest or motivate one to modify Yasukawa's non-encrypted (preview part) 46 to include hidden data, and even if one hid data in the non-encrypted (preview part) 46, it is readily apparent that Rhoads fails to suggest what kind of data should be hidden. Accordingly, it would be difficult to arrive at the claimed present invention by simply combining Rhoads and Yasukawa to provide the claimed present invention's, "***embedding user-specific authorization information***, containing information ***for accessing the encrypted digital content file***, as ***invisible information in the extracted preview sample to prepare a user-specific-authorization-information-embedded preview sample***" (e.g., claim 1). The fact that a combination of Rhoads and Yasukawa fails to disclose the claimed present invention is readily apparent, because the Office Action must rely on another reference Millsted.

Millsted discloses a method to send a preview of a sample digital content clip to an end user device from a web server. However, it does not disclose a method to synthesize the content itself and a sample preview that has invisible authorization information for accessing the encrypted portion of the content. In other words, Millsted like Rhoads discloses use of Watermarking technology, and discusses using the Watermarking process to apply copyright information to the content. However, Millsted fails to discuss other ranges of use of Watermarking technology. So, even if one assumes that Millsted and Rhoads can provide

suggestion or motivation to modify Yasukawa to apply Watermarking technology to information 36, both Millsted and Rhoads fail to provide suggestion or motivation to modify Yasukawa to apply Watermarking technology to Yasukawa's non-encrypted (preview part) 46 to provide the claimed present invention's, "***embedding user-specific authorization information***, containing information ***for accessing the encrypted digital content file***, as ***invisible information in the extracted preview sample to prepare a user-specific-authorization-information-embedded preview sample***" (e.g., claim 1). In other words, even if one applied Watermarking technology to Yasukawa's information 36, the Watermarking technology would be copyright information, and it would be difficult by one skilled in the art to arrive the claimed present invention's sample preview that has invisible authorization information for accessing the encrypted portion of the content.

The Office Action in page 5 provides that "It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of Yasukawa/Rhoads' with Millsted's distribution techniques, because this provides a system for tracking the use of digital data." However, contrary to the Office Action's combination and modification motivation rationale, the claimed present invention by "***embedding user-specific authorization information***, containing information ***for accessing the encrypted digital content file***, as ***invisible information in the extracted preview sample to prepare a user-specific-authorization-information-embedded preview sample***" (e.g., claim 1), provides (in an unlimiting example) one benefit of distributing a key for accessing encrypted content while substantially protecting the key and substantially reducing problems of loss of a key by a user.

So because a combination of Yasukawa, Rhoads and Millsted fails to disclose the claimed present invention, the Office Action relies on another fourth reference Stefik, which undermines the obviousness rationale to reject the claimed present invention. Stefik discloses embedding a watermark in a digital file that contains rights privileges. However, Stefik fails to disclose or suggest other range of uses of watermark technology. In other words, a review of entire Stefik reveals that Stefik discusses the "watermark data typically provides information relating to the owner of a document, the rights associated with that copy of the document and information relating to rendering event" (column 3, lines 22-39 and column 12, lines 10-51). However, Stefik fails to disclose or suggest the claimed present invention's sample preview that has invisible authorization information for accessing the encrypted portion of the content (i.e.,

"***embedding user-specific authorization information***, containing information ***for accessing the encrypted digital content file***, as ***invisible information in the extracted preview sample to prepare a user-specific-authorization-information-embedded preview sample***" (e.g., claim 1)). In particular, Stefik undermines the Office Action's obviousness rejection and motivation to combine and modify Yasukawa, Rhoads, Millsted and Stefik, because Stefik's column 12, lines 54-62, discuss "The next steps for the digital work are that it is published and distributed. During this process, the digital work is protected by the encryption and other security systems that are employed and the rights travel with the document." However, Stefik fails to contemplate the claimed present invention's sample preview that has invisible authorization information for accessing the encrypted portion of the content. In other words, Millsted and Stefik disclose a method to embed a digital watermark in a document. However, it would have been difficult for a person skilled in the art to assume that an encryption key is in a digital watermark in a preview sample of encrypted content.

Also, the Office Action in page 5 provides, "It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the distribution techniques of Yasukawa/Rhoads/Millsted with Stefik's usage rights because it provides a system for controlling the distribution of digital works." However, contrary to the Office Action's combination and modification motivation rationale, the claimed present invention by "***embedding user-specific authorization information***, containing information ***for accessing the encrypted digital content file***, as ***invisible information in the extracted preview sample to prepare a user-specific-authorization-information-embedded preview sample***" (e.g., claim 1), provides (in an unlimiting example) one benefit of distributing a key for accessing encrypted content while substantially protecting the key and substantially reducing problems of loss of a key by a user.

Yasukawa does not assume a method to embed a decryption key in a non-encrypted part as secret information and accordingly, it would have been difficult to employ the digital watermark technology as disclosed in Millsted and Stefik to reach the claimed present invention's idea. As mentioned above, it would have been difficult to combine Yasukawa, Rhoads, Millsted and Stefik.

Also, it would have been difficult to achieve the invention having the limitations disclosed in dependent claims 2-24.

CLAIMS 7-15

Claims 7-15 are rejected as being unpatentable over a combination of Yasukawa, Rhoads, Millsted, Stefik and a structure acknowledged by the Applicant.

A method to encrypt with a key which uses identification information unique to a user, such as HDD identification information, and a method to use an authorization information common to users are known in the art. However, because it would not have been easy to combine Yasukawa, Rhoads, Millsted and Stefik, it would have been difficult to combine these to achieve the claimed present invention, as follows:

Yasukawa is directed to a method to store an encrypted content in a recording medium and only constitutes a prior art of the present invention with respect to encryption of content. Also, a key sent from a distribution center or identification information unique to the device is used as a decryption key for decrypting encrypted information. When using a key separately from a distributed data, a conceivable problem is that a key gets lost, or that even an authorized user cannot use a digital content file when it is copied to another recording medium or is played on different devices.

In order to at least (among other problems) solve the above-mentioned problem, according the claimed present invention, the authorization information is embedded in the non-encrypted part as the invisible digital watermark, and the non-encrypted part is data synthesized with an encrypted part. Yasukawa does not recognize the above-mentioned problem(s) that if a key gets lost, or that even an authorized user cannot use a digital content file when it is copied to another recording medium or is played on different devices, and therefore it would have been difficult (i.e., there is no motivation) to combine Rhoads, Millsted, Stefik and the structure acknowledged by the Applicant to Yasukawa.

In view of the remarks, withdrawal of the rejection of pending claims and allowance of pending claims is respectfully requested.

CONCLUSION

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: July 7, 2005

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501